

In re Application of WITT et al.
Serial No. 09/560,788

Listing of the Claims:

1. (previously amended) In a computer system, a method comprising:
receiving information indicative of a possible change to a protected file; and
determining whether the possible change is valid by verifying the file, the
verifying performed by a verification mechanism, and if not valid, preventing the
possible change from being implemented including discarding the information
indicative of the possible change and returning a success to a component.
2. (original) The method of claim 1 wherein receiving information
indicative of a possible change includes receiving notification indicative of a change
to a protected file.
3. (original) The method of claim 1 wherein receiving information
indicative of a possible change includes receiving notification of a change to a file,
and accessing information to determine whether the file is protected.
4. (original) The method of claim 1 wherein preventing the change
includes overwriting a changed copy of the file with a valid copy of the protected
file.
5. (canceled)

In re Application of WITT et al.
Serial No. 09/560,788

6. (previously amended) The method of claim 1 wherein determining whether the possible change is valid by verifying the file includes obtaining cryptographic hash information of the changed file and comparing the cryptographic hash information against cryptographic hash information associated with the protected file.

7. (original) The method of claim 6 wherein comparing the cryptographic hash information includes accessing a catalog of information for protected files.

8. (previously amended) The method of claim 1 wherein determining whether the possible change is valid includes determining whether the file includes a signature.

9. (original) The method of claim 1 further comprising, monitoring files in a file system.

10. (previously amended) The method of claim 1 wherein preventing the possible change includes copying a valid copy of the protected file to a former location of the protected file.

11. (original) The method of claim 10 wherein copying a valid copy of the protected file includes finding a file having the same identity as the protected file.

In re Application of WITT et al.
Serial No. 09/560,788

12. (original) The method of claim 11 wherein finding the file having the same identity as the protected file includes accessing a cache.

13. (original) The method of claim 12 further comprising verifying the file having the same identity.

14. (original) The method of claim 11 wherein finding the file having the same identity as the protected file includes accessing a network.

15. (original) The method of claim 14 further comprising verifying the file having the same identity.

16. (original) The method of claim 15 wherein finding the file having the same identity as the protected file includes accessing a recorded medium.

17. (original) The method of claim 16 further comprising verifying the file having the same identity.

18. (canceled)

19. (previously amended) The method of claim 1 further comprising receiving information indicating that a protected file is about to be changed.

In re Application of WITT et al.
Serial No. 09/560,788

preserving a copy of the protected file, and wherein preventing the possible change includes overwriting a changed copy of the file with a copy of the protected file that was preserved.

20. (previously amended) A computer-readable medium having computer-executable instructions, comprising:

- (1) selecting a plurality of files as protected files;
- (2) receiving information indicative of a possible change to a protected file;
- (3) determining whether the file is an exception case, and
 - (a) if an exception case, allowing the change, or
 - (b) if not an exception case, determining whether the possible change is valid by verifying the file, the verifying performed by a verification mechanism, and
 - (i) if valid, allowing the possible change to be implemented;
- and
 - (ii) if not valid, preventing the possible change from being implemented; and
- (4) returning information indicative of a success.

21. (original) The computer-readable medium of claim 20 wherein receiving information indicative of a possible change includes receiving notification indicative of a change to a protected file.

In re Application of WITT et al.
Serial No. 09/560,788

22. (original) The computer-readable medium of claim 20 wherein receiving information indicative of a possible change includes receiving notification of a change to a file, and accessing information to determine whether the file is protected.

23. (previously amended) The computer-readable medium of claim 20 wherein preventing the possible change includes overwriting a changed copy of the file with a valid copy of the protected file.

24. (previously amended) The computer-readable medium of claim 20 wherein preventing the possible change includes discarding change data.

25. (canceled)

26. (previously amended) The computer-readable medium of claim 20 wherein allowing the possible change includes writing data saved via a copy-on-write process to the file.

27. (original) The computer-readable medium of claim 20 wherein determining whether the file is an exception case includes checking a security descriptor of the file.

In re Application of WITT et al.
Serial No. 09/560,788

28. (previously amended) The computer-readable medium of claim 20 further comprising providing a prompt before allowing a possible change.

29. (previously amended) The computer-readable medium of claim 20 wherein determining whether the possible change is valid includes obtaining cryptographic hash information of the changed file, and comparing the cryptographic hash information against cryptographic hash information associated with the protected file.

30. (previously amended) The computer-readable medium of claim 20 wherein determining whether the possible change is valid includes determining whether the file includes a signature.

31. (previously amended) A computer system, comprising,
a protected file,
a detection mechanism configured to determine when the protected file may be changed by a possible change,
a verification mechanism; and
a file protection service, the file protection service configured to receive a determination from the detection mechanism that the protected file may be changed, and further configured to communicate with the verification mechanism to verify whether the possible change is valid, and to prevent the possible change

In re Application of WITT et al.
Serial No. 09/560,788

from being implemented by discarding the possible change when the possible change is not valid.

32. (original) The computer system of claim 31 wherein the detection mechanism includes a mechanism for monitoring at least one directory for changes to at least one file therein.

33. (original) The computer system of claim 31 wherein the detection mechanism provides a notification to the file protection service as the determination mechanism that the protected file may be changed.

34. (original) The computer system of claim 31 wherein the file protection service accesses a data structure to determine whether the notification received from the detection mechanism corresponds to a protected file.

35. (original) The computer system of claim 31 wherein the file protection service is incorporated into a file system.

36. (canceled)

37. (previously presented) The computer system of claim 31 wherein the file protection service returns information indicative of a success.

In re Application of WITT et al.
Serial No. 09/560,788

38. (previously amended) The computer system of claim 31 wherein the verification mechanism verifies whether the possible change to a file is valid by comparing a cryptographic hash of the file contents against a cryptographic hash associated with a valid file.

39. (original) The computer system of claim 38 wherein the cryptographic hash associated with a valid file is maintained in a data structure including a cryptographic hash of the contents of at least one other protected file.

40-45. (canceled)

46. (previously amended) A computer system, comprising,
a protected file,
a detection mechanism configured to determine when the protected file may be changed by a possible change;
a verification mechanism; and
a file protection service, the file protection service configured to receive a determination from the detection mechanism that the protected file may be changed, and further configured to communicate with the verification mechanism to verify whether the possible change is valid, and to prevent the possible change from being implemented by locating valid data in a system cache and copying the valid data over changed data when the possible change is not valid.

In re Application of WITT et al.
Serial No. 09/560,788

47. (previously amended) A computer system, comprising,
a protected file,
a detection mechanism configured to determine when the protected file may
be changed by a possible change;
a verification mechanism; and
a file protection service, the file protection service configured to receive a
determination from the detection mechanism that the protected file may be
changed, and further configured to communicate with the verification mechanism to
verify whether the possible change is valid, and to prevent the possible change
from being implemented by locating valid data at a network share and copying the
valid data over changed data when the possible change is not valid.

48. (previously amended) A computer system, comprising,
a protected file,
a detection mechanism configured to determine when the protected file may
be changed by a possible change;
a verification mechanism; and
a file protection service, the file protection service configured to receive a
determination from the detection mechanism that the protected file may be
changed, and further configured to communicate with the verification mechanism to
verify whether the possible change is valid, and to prevent the possible change
from being implemented by locating valid data in a recorded medium and copying
the valid data over changed data when the possible change is not valid.

In re Application of WITT et al.
Serial No. 09/560,788

49. (previously presented) The computer system of claim 46 further comprising a scanning mechanism for causing a plurality of files to trigger the detection mechanism.